Department of Health and Human Services

The Centers for Medicare &
Medicaid Services
IT Modernization Program

CMS Security Services Guidelines

DRAFT

Version 0.7

March 31, 2005

Executive Summary

The Centers for Medicare & Medicaid Services (CMS) is in the process of modernization of CMS information technology (IT) capabilities. The future CMS enterprise architecture will consist of a three-Zone environment in which applications provide services to users, both internal and external, via web services. This three-Zone environment will make use of three zones—Presentation, Application, and Data—to ensure the integrity and protection of healthcare information. Users will employ web browsers to access web servers in the Presentation Zone. The web servers will be front-ends for CMS enterprise applications that run in the Application Zone. All application data will be stored in the Data Zone. The proposed CMS enterprise architecture will be dependent upon a baseline set of *enterprise* security services, as contemplated notionally in Figure ES–1. The baseline enterprise security services will be integrated into the three zones to provide a uniform level of security for all applications, data, and transactions in the CMS environment.

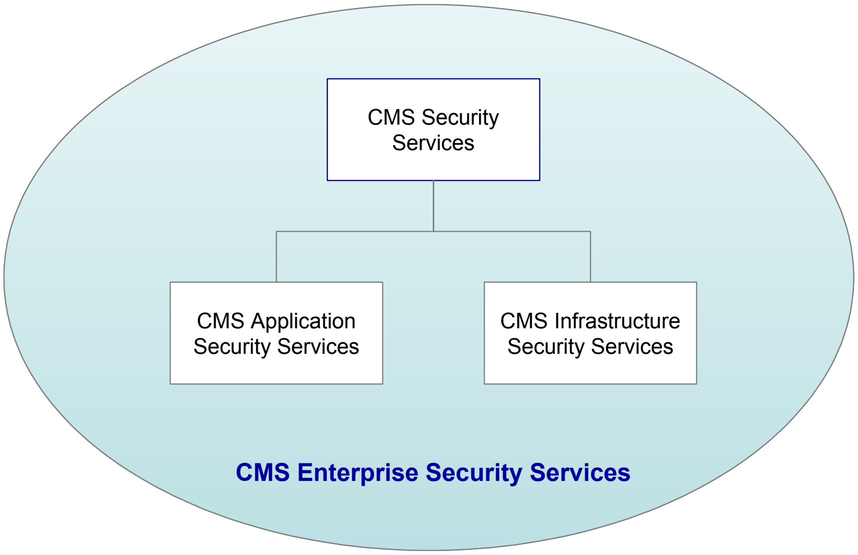
CMS Security Services
CMS Application Security Services
CMS Infrastructure Security Services
CMS Enterprise Security Services

Figure ES–1. Notional View of CMS Enterprise Security Services

The *CMS Security Services Guidelines* is a living document that describes the CMS vision of baseline security services and how they will be implemented on the CMS infrastructure. As CMS moves toward our target architecture and begins implementation, this document will change to reflect the adoption of new security technologies and refinement of existing security technologies. The goal is to ensure that security services are uniform and consistent for all CMS applications, data, and transactions.

Table of Contents

List of Figures

1. Introduction

The Department of Health and Human Services (HHS), through the Centers for Medicare and Medicaid Services (CMS), is in the process of an information technology (IT) modernization effort, expanding CMS capabilities by collecting and meeting new requirements, supporting more users, and building new applications. As part of the preparation for growth, increased automation, and technologic advances, CMS must comply with various federal regulations, including The Health Insurance Portability and Accountability Act (HIPAA), the E-Government Act, Federal Information Security Management Act (FISMA), and the Government Paperwork Elimination Act. HIPAA specifically mandates three categories of controls to secure electronic Protected Health Information (ePHI): Administrative, Physical, and Technical. Security programs should strike an appropriate balance among these three categories of controls. Technical safeguards support the baseline security services that will defend CMS from threats to Confidentiality, Integrity, and Availability.

The *CMS Security Services Guidelines* examine a number of technical controls that will enable CMS to establish common technical security safeguards that are consistent with HIPAA requirements. The recommended technical safeguards will be supported and complemented by administrative safeguards (such as policies, procedures, user training, etc.) as well as physical safeguards (such as physical access devices, alarms, cameras, etc.).

1.1 Purpose

The purpose of the *CMS Security Services Guidelines* is to:

- Establish common baseline security services for all CMS applications
- Enable CMS to meet mandated regulatory requirements
- Reduce exposures to security vulnerabilities by centralizing and standardizing security services
- Reduce recurring application-specific, security-related implementation costs
- Reduce the need for application developers to understand security in depth
- Provide integrated security services for CMS enterprise applications
- Automate application security through enterprise-wide security services.

As a result of the large volume of outsourcing required in recent years to automate CMS services, there has not been a unified approach to enterprise security. Individual projects and applications have employed various security mechanisms for the protection of confidential healthcare information. This document seeks to establish a common baseline of enterprise security services. This baseline of enterprise security services will provide a uniform level of confidentiality, integrity, and availability for all healthcare information created, received, processed, stored, or transmitted by CMS. In addition, a common set of security services will help ensure organization-wide uniformity in compliance with federal regulations and also reduce security-associated expenditures as individual applications no longer need to design and deploy application-specific security services.

The National Institute for Standards and Technology (NIST) is preparing new guidance the selection of appropriate security mechanisms. Documents, such as NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, is currently in draft form. When this guidance document is formally released, the *CMS Security Services Guidelines* will be reviewed and modified as necessary to ensure consistency.

1.2 Scope

This document identifies baseline technical security safeguards that are required for all new CMS information technology (IT) initiatives and programs. As legacy applications are updated and modernized, CMS will require their alignment with the baseline technical security safeguards described in this document.

1.3 Audience

This document is intended to guide CMS IT organizations and contractors who must comply with the finalized set of common technical security safeguards that will protect the CMS environment.

1.4 Document Organization

This document is organized into two sections and one major appendix. Section 2 introduces the CMS 3-Zone Architecture and describes Security Services required to safeguard ePHI. The recommended security services include Application Security Services and Platform Security Services.

2. Defining and Standardizing CMS Security Services

CMS requires common security services in the areas of:

- Identification and Authentication
- Authorization and Logical Access Control
- Cryptography (including non-repudiation)
- Audit
- Monitoring
- Perimeter Protection
- Malicious Code Protection.

These common security services will provide the core security mechanisms that applications will rely upon within the CMS infrastructure. CMS Security Services are divided into two categories: Application Security Services and Infrastructure Security Services. The *CMS Web Enabled Application Guidelines*, dated July 2003, provide additional guidelines on security services. The *CMS Information Security Acceptable Risk Safeguards (Draft version 1.1)*, dated March 14, 2003, provide Security Standards for System Security levels of Low, Moderate and High.

2.1 CMS 3-Zone Architecture

CMS will be migrating to a web services environment in which services for internal and external users/customers will be provided by web applications. To support the new environment, a three-Zone architecture, as shown in Figure 1, has been developed to comply with HIPAA. By layering the infrastructure into three zones—the Presentation Zone, Application Zone, and Data Zone, CMS can supply more protection to infrastructure components located in inner zones. The outermost or *Presentation Zone* will only support web servers. The middle or *Application Zone* will support each application's business logic. The innermost or *Data Zone* will also include mainframe databases used to store all CMS application data. This architecture provides an increased degree of security since its multiple zones isolate protected healthcare data.

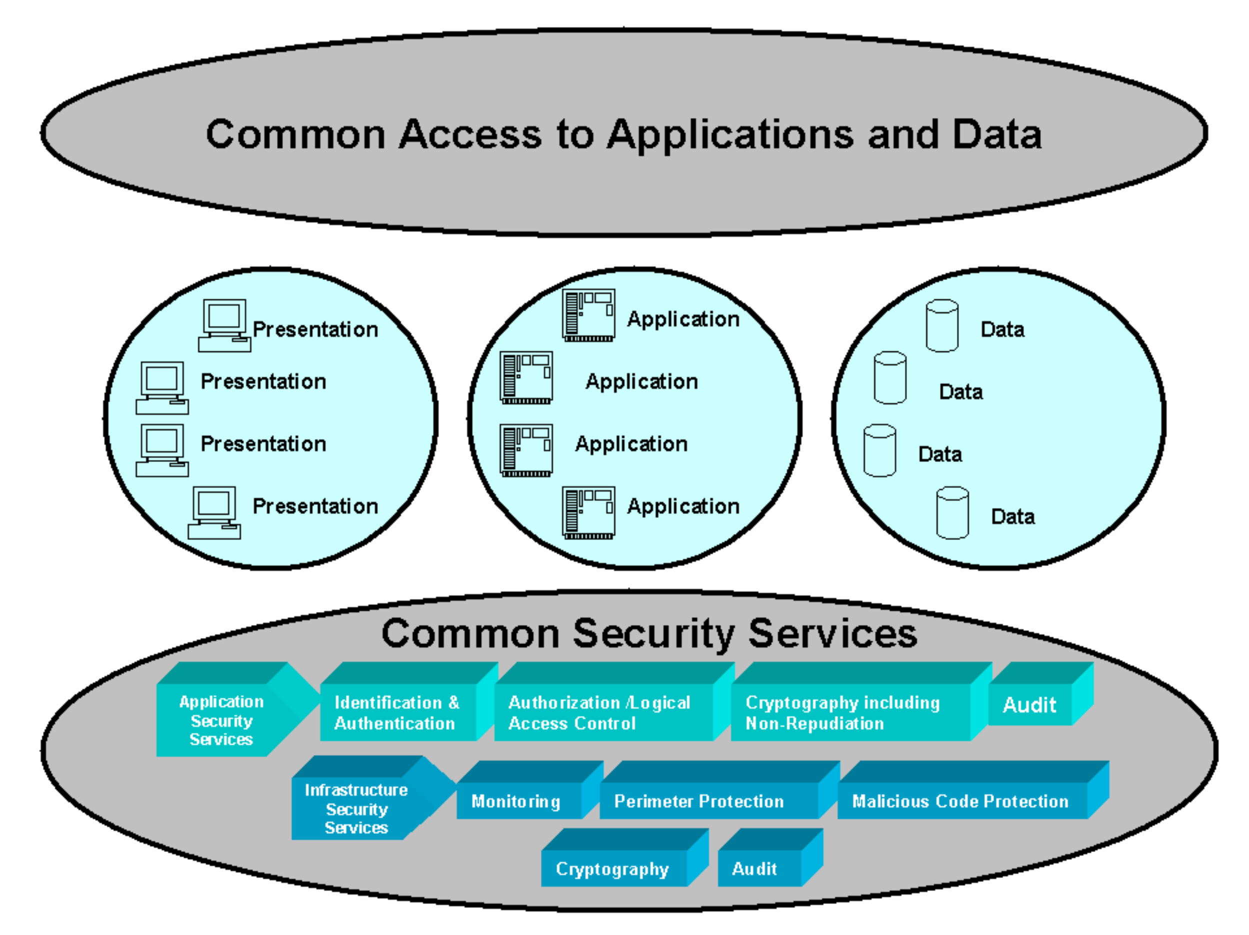
Common Access to Applications and Data
Presentation
Presentation
Presentation
Presentation
Application
Application
Application
Application
Data
Data
Data
Data
Common Security Services
Application Security Services
Identification & Authentication
Authorization /Logical Access Control
Cryptography including Non-Repudiation
Audit
Infrastructure Security Services
Monitoring
Perimeter Protection
Malicious Code Protection
Cryptography
Audit

Figure 1. Overview of the CMS 3-Zone Architecture Application Security Service Requirements

Application security services are those security services that are typically visible to the application developer. These services are most effective when they are transparent to the end user.

Enterprise applications should make use of the standard security services provided by CMS, and should understand security implicitly. In cases where commercially available applications are used, applications should be configured with advanced security controls that comply with CMS enterprise security policies for access control and handling. Today, CMS Security Services make the provisions that applications use to meet their respective security requirements. In the future, the CMS Application Security Services will be used to intercept client requests and enforce security policies in a manner that is transparent to the applications.

2.1.1 Application Sensitivity Level Requirements

CMS has established Identification and Authentication (I&A) requirements according to application sensitivity levels (low, medium, and high). The application sensitivity levels are based on levels of user privileges and are defined as follows:

- **Low.** For applications whose sensitivity is rated as *Low*, anonymous access will be permitted. These types of systems consist of World Wide Web (WWW) pages that provide static information to the general public about CMS and CMS programs. Users who use applications with low sensitivity levels will have access to non-sensitive information.
- **Medium.** For applications whose sensitivity is rated as *Medium*, username and password will be required. Users who use applications with medium sensitivity levels will have access to moderately sensitive information.
- **High.** For applications whose sensitivity is rated as *High*, both username/password and an RSA SecureID hardware token or digital certificate will be required. Users who use applications with high sensitivity levels may have access to highly privileged information.

2.1.2 Identification and Authentication

Identification and Authentication is a security service that establishes and verifies the identity of an entity on an information system. I&A forms the basis for most authorization and access controls. Individual users are typically the “entities” that are authenticated, although system entities may be authenticated as necessary. All CMS applications should rely on the CMS I&A security service to accomplish the authentication of the users and system entities that connect to it. CMS will use the Sun Java Enterprise System (JES) for I&A security services.

There are generally three recommended techniques used to perform authentication of user entities:

- Requiring something users *know* (i.e., passwords)
- Requiring something users *have* (i.e., tokens)
- Requiring something users are (i.e., biometrics).

These authentication techniques can be combined to provide additional degrees of confidence using multiple-factor authentication. For example, users requiring access to sensitive data could be required to perform dual-factor authentication by requiring a password and token. For access to extremely sensitive data, CMS users, that include employees, contractors, or business partners, could be required to provide three-factor authentication in the form of a password, token, and fingerprint scan.

Enterprise identity management is also an integral part of I&A. Identity management provides a common process to provision user identification. It is important that users have only one username and associated password. Currently, it is common for IT users in large organizations to juggle multiple usernames and associated passwords. Users with multiple logins and passwords increase the total cost of ownership for the infrastructure by producing extra work in the form of high volumes of calls to the helpdesk for the purpose of resetting passwords. It's often the case that users with multiple logins and passwords create the potential for increased risk exposure since they frequently keep a paper record of their accounts and passwords.

Effective identity management solutions include tools that help network administrators identify numerous usernames/passwords that are associated with individuals and effect a replacement with a single enterprise username/password.

In a multi-tiered environment such as CMS, users are usually authenticated at the Web Server. In some cases, a more sensitive application may require additional authentication after the user has already completed an initial I&A process. In such cases, the CMS Security Services will provide the means for the application to request additional authentication.

All individuals will be assigned unique identifiers. Shared user identification creates undue security risks and should not be used. Access protection measures must provide assurance of individual accountability by means of I&A of each user.

2.1.2.1 I&A Enhancements

By using Strong User Authentication (SUA) and Single Sign-On (SSO), CMS can significantly enhance application security. SUA, such as hardware or software tokens, and SSO combine to simplify and strengthen user access controls and add protection to users and sensitive data. Some CMS applications will require the use of SSO solutions.

SSO solutions have the ability to integrate with more sophisticated broker-based authentication methods, including such hardware and software tokens as password tickets, smart cards, and password tokens. SSO solutions provide software development kits to develop custom applications, embed SSO in their environment, and extend the capabilities of an SSO product. Application Programming Interfaces (APIs) can be used for developing applications that use the services provided by the SSO solution. Applications must make use of I&A services provided by the CMS Enterprise Security Services from well-established vendor products.

The user-provisioning solution will store answers to user-selected personal challenge-response questions. These questions and answers will form the basis of automatic password resets for users who have forgotten their passwords. A user who has forgotten his/her password will enter the userid and answer the questions selected during registration. If the answers are correct, a temporary password will be sent via email to the user’s email account of record. This will alleviate the burden on CMS support personnel to answer username/password requests.

2.1.2.2 Web Services I&A

In the near future, CMS applications will become accessible via web services. This will allow remote users distributed throughout the U.S. to connect to CMS via the Internet using their Internet Service Provider. As more applications are made available through web services, CMS will migrate large classes of remote users to Internet access from their current access via modem pools located at Value Added Networks (VANs). The only client software required will be a web browser. Users will employ web browsers to securely connect to CMS web servers using [HyperText Transport Protocol (HTTP) Secure]. After successful SSO validation, users will be able to access CMS web-enabled applications for which they have authorization.

2.1.2.3 Compliance with Federal Mandates

CMS will investigate ways to comply with the goal of the E-Government Act to provide citizens the ability to access government services and information within three "clicks" over the Internet. There are significant challenges in accomplishing I&A of citizens who have no prior relationship with CMS. The General Services Administration (GSA) has released a draft E-Authentication policy that outlines four levels of assurance against which agencies must align transactions and services by September 15, 2005. Both the E-Government Act and the draft E-Authentication policy will require CMS to investigate innovative ways to meet these goals while affording appropriate levels of security to ePHI.

To support these initiatives, Knowledge-Based Authentication (KBA) will be evaluated as an option since costs associated with traditional I&A mechanisms for the population as a whole are too costly. It is anticipated that the CMS I&A solution must support these KBA techniques.

KBA can reduce costs associated with identifying and authenticating prospective users who can come from the population as a whole. KBA differs from traditional I&A techniques because userids and shared secrets are not established beforehand. KBA I&A techniques first seek to verify claimed user identities exists and then attempt to prove users are in fact who they claim to be. For example, a citizen requesting access to a CMS web service must provide "wallet-based" information such as name, address, and phone number. Online databases such as one of the three public credit bureaus can be used to verify that a person exists with that *name*, at that *address*, and possessing that *phone number*. Once this has been verified, it remains to be confirmed that the claimed identity belongs to the person requesting the transaction. This is more challenging than traditional I&A mechanisms because no shared secret (password) exists between the two parties. However, the user and CMS may have some shared non-public information that could be used. For example, a citizen requesting the status of a medical appeal could be asked to enter the original amount of the appeal. This information would provide a weak but sufficient level of authentication to permit the citizen's access to the current status of the appeal.

Another option for verifying and validating identities would be to use third-party commercial services that provide standardized levels of authentication using publicly available databases. Commercial companies may be able to use public credit information and possibly banking information in some way to validate and authenticate citizens on the Internet. If such commercial services evolve, the CMS I&A process will require a mechanism to receive third-party authentication assertions such as Security Assertion Markup Language (SAML). The CMS I&A solution will have to be sufficiently flexible to allow for KBA techniques once they are established.

2.1.3 Authorization/Logical Access Control

Authorization is the process of determining whether an entity should be permitted to execute a function or access a resource. Logical access controls are mechanisms designed to ensure that the ability to execute functions and access resources is limited to authorized entities. Access controls for applications prevent unauthorized access to sensitive data and programs that are stored or transmitted electronically. Authorization/access control can be based upon user identity, role membership, group membership, or some other information known to the system.

Authorization/access controls provide more granular protection of ePHI confidentiality, integrity, and availability by supporting the principles of least privilege and separation of duties.

As required for I&A, applications are required to make use of authorization/access control services provided by the CMS Enterprise Security Services from well-established vendor products. The access control framework provided by CMS Enterprise Security Services will provide the ability to determine which entities shall be allowed to perform what action, when, from where, in what order, and in some cases, under what relational circumstances.

In a large enterprise, the Authorization Service must be scalable. The CMS Authorization Service supports approaches, such as role-based access control, to allow many individual users to be grouped together under a single role. The access control rules are defined for the role, not for each individual user. The Authorization Service provides a means for the application to determine the privileges of the entity that invoked it (for instance, the role of the user who caused the application to be invoked). This is necessary to enable the application to make context-specific decisions.

Access controls can be defined for any resource. In a multi-tier J2EE (Java 2 Platform, Enterprise Edition) environment such as CMS, access controls are generally needed at a minimum for web server, portal, and application server resources. Examples of resources that may require controlled access include URLs on a web server, J2EE web applications [servlets, Enterprise Java Beans (EJBs), HTML (Hypertext Markup Language) pages, image files], and Java naming and directory interface.

2.1.4 Cryptography

The CMS Security Services infrastructure will provide cryptographic services that will enable applications to make use of encryption and digital signatures. A Public Key Infrastructure (PKI) will issue X.509 certificates that will enable entities (applications and users) to encrypt data and use digital signatures. A well-established Certificate Authority (CA) product will issue PKI certificates to users and enterprise application servers. Applications designated as Medium or High risk (for data sensitivity) shall be capable of using X.509 certificates to encrypt all data transmitted across all component zone boundaries. In addition, Low-, Medium-, and High-risk applications will make use of digital signatures when appropriate.

The CMS CA will provide the ability to securely backup (escrow) private keys used for encryption. This will provide a mechanism to “re-issue” private keys to users who have forgotten their private key passwords or whose private keys have been destroyed. Private keys used for signing will not be escrowed for legal reasons. CMS will issue a pair of certificates to users, one for encryption and one for signing. This is a common practice in federal government agencies.

The CMS CA will also support a number of mechanisms for certificate revocation since this is an area where PKI technology has not yet matured. When the CMS PKI architecture is finalized, CMS will decide whether On-line Certificate Status Protocol (OCSP) or Certification Revocation Lists (CRLs) will be employed.

S/MIME (Secure/Multipurpose Internet Mail Extensions) provides a consistent way to send and receive secure MIME data. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications:

- Authentication
- Message integrity
- Non-repudiation of origin (using digital signatures)
- Privacy and data security (using encryption).

S/MIME can be used by traditional mail user agents (MUAs) to add cryptographic security services to mail that is sent, and to interpret cryptographic security services in mail that is received. However, S/MIME is not restricted to mail; it can be used with any transport mechanism that transports MIME data, such as HTTP. As such, S/MIME takes advantage of the object-based features of MIME and allows secure messages to be exchanged in mixed-transport systems.

S/MIME also can be used in automated message transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software-generated documents and the encryption of FAX messages sent over the Internet.

The CMS CA will also have the functionality required to support the Federal Bridge Certification Authority (FBCA). The FBCA provides a mechanism for PKIs in various federal agencies to interoperate. This requires that the CA be capable of cross-certification. Cross-certification is where the CA can issue a cross-certificate to another agency's CA to extend trust to that agency's subscribers and associated applications. Cross-certification also requires use of client applications capable of building certification paths of certificates through cross-certificates stored in directories. In particular, the CA and client applications must support the nameConstraint, certificatePolicies, and policyMapping extensions. Current policy and interoperability information is available at http://www.cio.gov/fpkisc/fpki_docs.htm.

Present-day network connectivity and technologies provide CMS opportunities to conduct more business transactions electronically in a paperless environment. To be successful, it is critical that these transactions be auditable and have comparable legal status to paper transactions. Digital signatures based on X.509 certificates provide this capability by offering two features. First, they provide cryptographic proof that a signed file has not been altered since it was signed. Second they prove the signer's identity. The Digital Signatures Act of 2000 establishes the legal validity of digital signatures. CMS policies on certificate issuance will be sufficiently stringent that X.509 digital signatures will provide legal non-repudiation. Legal non-repudiation refers to the ability of digital signatures to stand up in court because stringent organizational policies enforce rigorous certificate issuance procedures. Employment of digital signatures can provide a secure way to automate numerous processes that are still done manually. CMS will explore the use of digitally signed forms once the CMS PKI is in place.

2.1.5 Audit

The CMS Security Services infrastructure will provide a security audit service for all applications. The Application Security Services themselves generate audit data (e.g., .recording security-relevant information about authentication or access control decisions). In addition, the Application Security Services provide an interface for applications to generate application-specific audit information. The selection of the appropriate events to be audited should be determined jointly by the application developers and the CMS Security Group. Applications should be able to detect all application-specific security-relevant events, collect security-relevant event data such as time-stamp and identity of the responsible entity, and transmit the event data to the CMS Audit Service.

The CMS Audit Service will consolidate application audit data into a centralized audit log repository for review and secure storage. CMS plans to implement Security Information Management (SIM) technology to consolidate and centralize the security-relevant event data. SIM aggregates security-relevant event data from many different types of security devices [e.g., Intrusion Detection Systems (IDS), firewalls, routers, Servers, Syslogs]; normalize the security-relevant event data; correlate it; and present it within a single, integrated display. It processes security-relevant event data produced by devices in a near real-time manner and boosts security analyst effectiveness by streamlining the process of security event/alarm investigation and automating manual, time-intensive tasks.

2.2 CMS Infrastructure Security Services

Infrastructure Security Services are services available to applications operating on the CMS infrastructure. Application developers must be aware of these infrastructure security services and ensure that their applications can make use of them when required. The CMS infrastructure security services enforce CMS security policies to protect CMS infrastructure, applications, and data.

2.2.1 Perimeter Protection

Firewalls are often discussed in the context of providing perimeter protection for an enterprise infrastructure against connections to the Internet. Firewalls control the flow of traffic between networks because they are implemented as single points through which all communications must pass. Firewalls may also be employed in internal networks to restrict connectivity to more sensitive areas.

Firewalls will provide security between CMS network zones by limiting the types of activities that occur between them. Every connection between network zones in CMS must pass through firewalls. To provide maximize protection, no two consecutive firewalls will have the same ports open. Enterprise applications must take CMS firewall configurations into consideration during the design phase to ensure planned application functionality is not in conflict with enterprise firewall configuration policies. For example, firewalls that protect the presentation zone will only allow traffic on port 80 (HTTP), port 443 (HTTPS), and port 53 (DNS). Applications requiring ports other than CMS-allowed ports will have to obtain authorization in writing from the CMS Chief Architect. In addition, CMS firewalls will filter mobile code to prevent high-risk mobile code technologies from passing from one zone to another.

Firewalls have the ability to proxy services between different network zones. Proxy services prevent any direct Transmission Control Protocol (TCP)/Internet Protocol (IP) connections between entities in different zones. Firewalls also generally use Network Address Translation (NAT) to present one internal IP addresses to external entities.

CMS firewalls will provide the following protection services:

- Bi-directional packet filtering
- Stateful packet inspection
- Proxy Services
- Network Address Translation.

2.2.2 Monitoring

Intrusion Detection Systems will provide security by monitoring network events occurring in each of the three zones and detecting signs of intrusions. Intrusions are defined as attempts to perform unauthorized actions or bypass security controls. Intrusions can be caused by outside attackers accessing the system, authorized users attempting to gain additional privileges for which they are not authorized, or users abusing privileges for which they are authorized. IDSs use two different approaches for detecting attacks. A signature-based approach identifies events or sets of events that match pre-defined patterns of known attacks. An anomaly-based approach establishes normal activity profiles for users and assumes that user profiles having significant statistical deviations from these constitute an attack. CMS IDSs will provide protection by monitoring network traffic for:

- Attack Signatures
- Protocol Anomalies
- Traffic Anomalies.

CMS IDS services will be provided by ISS RealSecure.

Intrusion Prevention Systems (IPSs) are the next evolution of IDSs. Intrusion prevention systems attempt to stop intrusions before data is compromised or damage is done. Unlike an IDS that passively monitors network traffic, an IPS resides inline like a firewall and can intercept and block packets from an intrusion in real time. Unfortunately, IPSs may cause operational issues if detection of intrusion events is not accurate and legitimate activities are blocked. CMS will not make use of network IPSs until the state of the technology matures.

Vulnerability scanning adds security by verifying the network, system, and application security controls and configurations. Vulnerability scanning includes checking open ports, trapdoors, system and application scripts, and operating system configurations and patch levels. Automatic

Vulnerability Remediation, or Patch Management, eliminates identified vulnerabilities, wherever possible, by installing appropriate security patches and modifying configurations.

2.2.3 Malicious Code Protection

Virus protection for CMS will be provided by McAfee desktop and server virus scanning products. In addition to virus scanning on the CMS infrastructure, workstations that have the ability to connect to the Internet will be required to have desktop virus scanning installed and enabled. CMS will require that users download new virus signature files at least once a week.

2.2.4 Cryptography

The CMS Security Services infrastructure will provide cryptographic services to all applications that require them, including symmetric and asymmetric encryption, digital signatures, and such cryptographic infrastructure functions as key generation, distribution, storage, and management.

2.2.4.1 Secure Web Services

CMS web servers and web browsers will make use of Secure Socket Layer (SSL) version 3 or Transport Layer Security (TLS). In addition, only cryptographic modules validated as FIPS 140-1 or 140-2 compliant will be permitted. Symmetric encryption for SSL and TLS must use key lengths of 128-bit or greater. Configurations of CMS servers and client applications shall prevent use of algorithms that do not support key lengths of 128-bit or greater. To connect to CMS Secure Web Services requires Microsoft Internet Explorer Version 5.5 or higher and Netscape Version 4.5 or higher. Applications that use Digital Signatures must allow signatures that are compliant with the Digital Signature Standard per FIPS 186.

CMS web servers located in the Presentation Zone will make use of SSL accelerators. SSL accelerators relieve the encryption processing burden from web servers and enable load balancing among several web servers. In addition, SSL accelerators allow IDS monitoring of HTTPS traffic that would otherwise not be possible.

2.2.4.2 Secure Transport

Wide Area Networks (WANs) traditionally have been implemented using leased lines employing Frame Relay or Asynchronous Transfer Mode (ATM) between remote sites. In recent years, however, high-speed Internet connections to enterprise networks have enabled Virtual Private Networks (VPNs) to be established over external IP networks such as the Internet. This has produced significant cost reductions for connectivity to remote sites. VPN tunneling across the Internet requires robust encryption as well as authentication of the remote end. IPSec [Internet Protocol (IP) Security] is the most widely used tunneling protocol because it provides both of these features. In addition to encryption, other aspects of physical networking such as Quality of Service (QoS), reliability, and management are concerns with virtual networks as well.

VPNs are used to provide three different types of secure connectivity. They can link office Local Area Networks (LANs) in separate geographic areas to form a WAN. They can be used to allow remote users to dial-in or connect to an enterprise LAN. They can also be used to provide a secure channel directly to client workstations. The CMS VPN solution will primarily provide connectivity from the central office to regional offices and contractor sites. CMS allows 85,000 remote access users, 20,000 Medicare contractor staff, and 5,000 Medicaid state agency staff on external platforms to remotely connect to the enterprise via the CMS Systems Network Architecture (SNA). The CMS VPN solution should be capable of providing secure communications directly to client computers should the need arise in the future. CMS may make use of a VPN concentrator product that provides both SSL and IPSec-based connectivity to best fit their diverse remote access end-user requirements.

2.2.5 Audit Consolidation

Application audit logs will be consolidated to a centralized audit log repository for review and secure storage. In the event of a security incident, it will be possible to use this centralized service to establish a chain of evidence.

Acronyms

ATM	Asynchronous Transfer Mode
CA	Certification Authority
CMS	Centers for Medicare and Medicaid Services
DAC	Discretionary Access Control
DB2	DataBase 2
ePHI	electronic Protected Health Information
EJB	Enterprise Java Beans
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
I&A	Identification and Authentication
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security
J2EE	Java 2 Platform, Enterprise Edition
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
PKI	Public Key Infrastructure
QOS	Quality of Service
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAML	Security Assertion Markup Language

SIM	Security Information Management
SNA	System Network Architecture
SSL	Secure Socket Layer
SSO	Single Sign-On
SUA	Strong User Authentication
TLS	Transport Layer Security
VAN	Value Added Network
VPN	Virtual Private Network
WAN	Wide Area Network

List of References

1. The Health Insurance Portability and Accountability Act (HIPAA).
2. E-Government Act.
3. Federal Information Security Management Act (FISMA).
4. E-Authentication Guidance for Federal Agencies.
5. Government Paperwork Elimination Act.
6. National Institute of Standards and Technology (NIST) Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure.*
7. NIST Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2.*
8. NIST Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication.*
9. Draft NIST Special Publication *800-53, Recommended Security Controls for Federal Information Systems.*
10. Federal Information Processing Standards (FIPS) Publication 199, Standard for Security *Categorization of Federal Information and Information Systems.*